MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito
Ingeniería Social

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Diciembre 2018

Sobre MILE-SEC

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

MILESEC E.I.R.L, es una empresa de capitales Peruanos fundada en el año 2017, la cual está netamente dedicada a brindar servicios de capacitación, relacionados con las áreas de seguridad de la información y tecnologías de la información, tales como; Pruebas de Penetración (Penetration Testing), Hacking Ético (Ethical Hacking), Evaluación de Vulnerabilidades (Vulnerability Assessment), Forense de Computadoras (Computer Forensics) y Forense Digital (Digital Forensics). Brinda servicios de consultorías especializadas en todas las áreas mencionadas.


http://www.mile-sec.com/


informes@mile-sec.com / mileseceirl@gmail.com


https://www.facebook.com/mileseceirl/

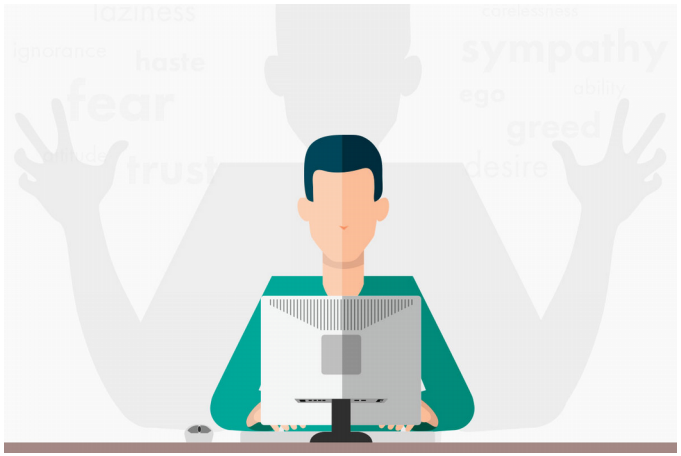

https://twitter.com/mileseceirl


https://www.linkedin.com/in/milesec/

Temario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

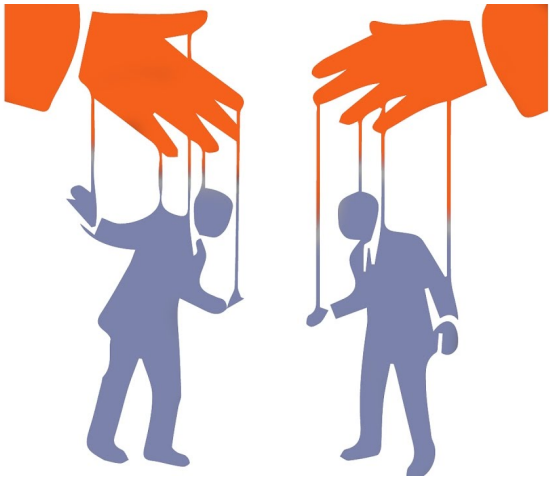
- Introducción a la Ingeniería Social
- Iniciar las Pruebas de Ingeniería Sociales
- Porque los Atacantes utilizan Ingeniería Sociales
- Entender las Implicaciones
- Construir Confianza
- Explotar las Relaciones
- Realizar Ataques de Ingeniería Social
- Buscar Información
- Medidas Correctivas de Ingeniería Social
- Políticas
- Concientización y Entrenamiento del Usuario



Ingeniería Social

La ingeniería social toma ventaja del enlace más débil en cualquier defensa de seguridad de la información en la organización; las personas. La ingeniería social es “Hacking a las personas”, e involucra explotar maliciosamente la natural confianza del ser humano para obtener información la cual puede ser utilizada para ganancia personal.

La ingeniería social es uno de los “hacks” más duros para penetrar, porque requiere valentía y destreza para un extraño sienta confianza. Es también de lejos, lo más difícil de proteger, porque las personas quienes toman sus propias decisiones de seguridad están involucradas.



Introducción a la Ingeniería Social

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

En una escenario de ingeniería social, aquellos con mala intención suplantan a alguien mas para ganar información a la cual de otra manera no podrían acceder. Luego toman la información obtenida desde las victimas, y causan estragos en los recursos de la red, roban o borran archivos, o incluso cometen espionaje corporativo, o alguna otra forma de fraude contra la organización atacada. La ingeniería social es diferente de las vulnerabilidades de seguridad física, como el ver sobre los hombros, o buscar en los basureros, pero los dos tipos de hacking están relacionadas y frecuentemente se utilizan juntos.

Algunos ejemplos de ingeniería social:

- Personal de apoyo
- Proveedores
- Empleados
- Correos electrónicos “Phishing”

Iniciar las Pruebas de Ingeniería Sociales

La ingeniería social es un arte y una ciencia. La ingeniería social requiere grandes conocimientos para ser realizado como un profesional en seguridad, y es altamente dependiente de la personalizad, además de un conocimiento global sobre la organización.

La ingeniería social pude dañar el trabajo de las personas y sus reputaciones, e información confidencial puede ser expuesta. Esto es especialmente cierto cuando se realizan pruebas de phishing. Se deben planificar las cosas y proceder con precaución.

Se pueden realizar ataques de ingeniería social en millones de maneras. Desde caminar a través de la puerta principal diciendo ser alguien quien no se es, hasta lanzar una campaña de phishing a través de correos electrónicos.

Se puede tercerizar las pruebas de ingeniería social, o incluso asignarlo a un colega de confianza.

Porque los Atacantes utilizan Ingeniería Sociales

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Las personas utilizan ingeniería social para irrumpir dentro de los sistemas y obtener información, pues frecuentemente es la manera más sencilla de obtener lo buscado. Es preferible alguien abra la puerta de la organización, en lugar de irrumpir físicamente arriesgándose a ser atrapado. Las tecnologías de seguridad como firewalls y controles de acceso, no detendrán a un ingeniero social con determinación.

Muchos ingenieros sociales realizar sus ataques lentamente para evitar sospechas. Los ingenieros sociales obtiene fragmentos e información a través del tiempo, y utilizan esta información para crear una imagen amplia de la organización la cual intentan manipular. Aquí radica uno de sus mayores activos. No se tiene más a tiempo, y se tomarán la cantidad apropiada para asegurar los ataques sean exitosos. Alternativamente, algunos ataques de ingeniería social pueden realizarse con una llamada telefónica rápida o correo electrónico. Los métodos utilizados dependen del estilo y las habilidades del atacante. De cualquier manera se está en desventaja.

Entender las Implicaciones

Muchas organizaciones tienen enemigos quienes quieren causar problemas a través de ingeniería social. Estas personas pueden ser empleados actuales o anteriores quienes buscan venganza, competidores quienes desean una ventaja, o Hackers intentando demostrar su valía.

Ingenieros sociales efectivos pueden obtener la siguiente información:

- Contraseñas de usuario
- Insignias de seguridad o llaves del edificio, e incluso de la sala de computadoras
- Propiedad intelectual como especificaciones de diseño, código fuente, u otra documentación de investigación y desarrollo
- Reportes financieros confidenciales
- Información privada y confidencial de los empleados
- Información identificable personalmente (PII) tales como registros médicos e información de tajetahabientes
- Lista de clientes y prospectos de ventas

Construir Confianza

Confianza – tan difícil de ganar pero tan fácil de perder. La confianza es la esencia de la ingeniería social. La mayoría de personas confían en otras hasta una situación los obliga a no hacerlo. Las personas quieren ayudarse mutuamente, especialmente si se puede construir confianza y la solicitud de ayuda parece razonable. La mayoría de personas quieren ser jugadores en el lugar de trabajo y no se percatan de aquello lo cual puede suceder si se divulga demasiada información hacia una fuente en la cual no se debe confiar. Esta confianza permite a los ingenieros sociales cumplir sus objetivos. De hecho, construir una profunda confianza frecuentemente toma tiempo. Los ingenieros sociales astutos pueden obtenerlos en minutos u horas. ¿Cómo lo hicieron?.

- Simpatía
- Credibilidad

Explotar las Relaciones

Engaño a través de palabras y acciones. (y a través de tecnologías)

- Actuar de manera demasiado amistosa o ansiosa
- Mencionar nombres de personas prominentes dentro de la organización
- Presumir de autoridad dentro de la organización
- Amenazar con reprimendas si no se cumplen las solicitudes
- Actuar nervioso cuando se le pregunta
- Demasiado énfasis en los detalles
- Experimentar cambios fisiológicos
- Aparecer apresurado
- Negarse a dar información
- Información voluntaria y responder preguntas no formuladas
- Conocer información la cual un extraño no debería tener
- Usar lenguaje interno o jerga como un externo conocido
- Hacer preguntas extrañas
- Palabras mal escritas en las comunicaciones

Realizar Ataques de Ingeniería Social

El proceso de ingeniería social es en realidad bastante básico. En general, los ingenieros sociales descubren los detalles sobre las personas, procesos de las organización, e información de los sistemas para realizar sus ataques. Con esta información se conoce aquello a perseguir. Los ataques de ingeniería social típicamente se realizan en cuatro simples pasos:

- Realizar investigación
- Construir confianza
- Explotar las relaciones por información a través de palabras, acciones o tecnología
- Uso de información obtenida para propósitos maliciosos

Estos pasos pueden incluir numerosos subpasos y técnicas, según el ataque a realizar.

Buscar Información

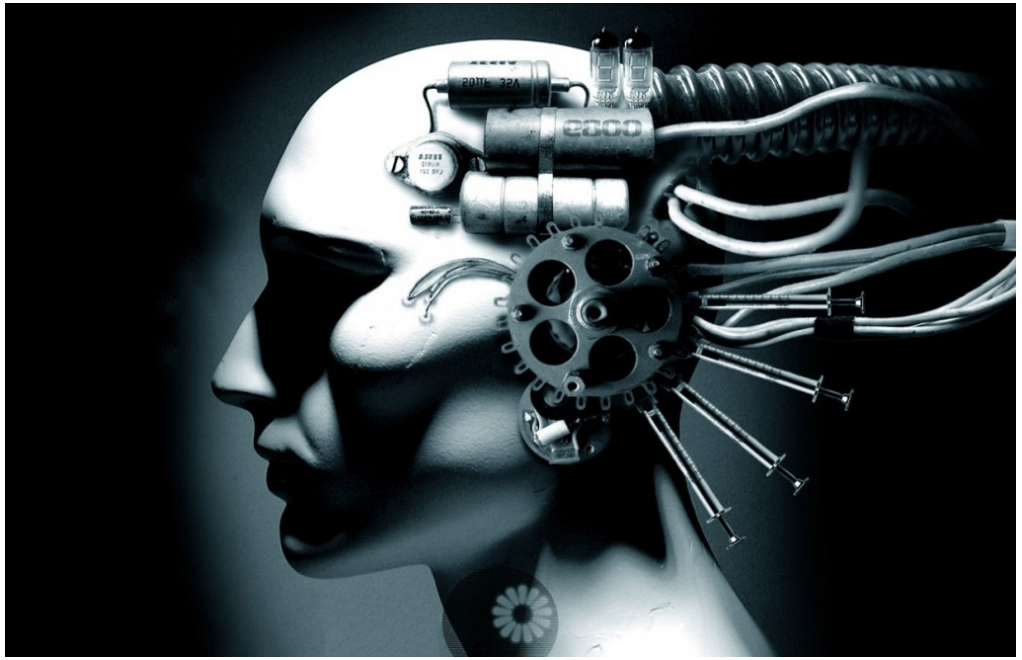
MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Después de los ingenieros sociales tienen un objetivo en mente, típicamente se comete un ataque mediante la recolección de información pública sobre las victimas. Muchos ingenieros sociales adquieren información lentamente a través del tiempo para no levantar sospechas. La recopilación de información obvia es un indicio cuando se defiende contra la ingeniería social.

- Utilizando Internet
- Buscar en la basura. Listas de teléfonos internos, gráficos organizacionales, manuales de empleados, diagramas de red, listas de contraseñas, notas de reuniones, registros de clientes, correos impresos.
- Sistemas telefónicos. Teléfonos residenciales, teléfonos de la empresa, servidores VoIP.
- Correo electrónicos Phishing. Tener errores tipográficos, contener saludos genéricos y firmas de correos electrónicos, pedir al usuario haga clic directamente en un enlace, solicitar información sensible.

Medidas Correctivas de Ingeniería Social

Se tienen únicamente algunas buenas líneas de defensa contra la ingeniería social. La ingeniería social pondrá a prueba las defensas en capas. Incluso con fuertes controles de seguridad, un usuario ingenuo o inexperto puede permitir el ingeniero social ingrese hacia la red. Nunca se debe subestimar el poder de los ingenieros sociales, y el de sus usuarios, además de ayudarlo a encontrar su camino.



Políticas

Las políticas específicas ayudan a evitar la ingeniería social a largo plazo en las siguientes áreas.

- Clasificar información para los usuarios no tengan acceso hacia ciertos niveles de información no necesaria.
- Configuración del ID de usuario al contratar empleados o proveedores.
- Establecer el uso aceptable de las computadoras, y los usuarios estén de acuerdo por escrito.
- Eliminar IDs de usuarios para los empleados, proveedores, y consultores quienes no trabajen más en la organización.
- Establecer y restablecer frases de paso fuertes
- Responder rápidamente hacia incidentes de seguridad, tal como comportamiento sospechoso e infecciones de Malware conocidas.
- Manejar adecuadamente información propietaria y confidencial.
- Acompañar a los invitados alrededor del edificio.

Concientización y Entrenamiento del Usuario

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Una de las mejores líneas de defensa contra la ingeniería social es entrenar a los empleados a identificar y responder a los ataques de ingeniería social. La concientización del usuario comienza con el entrenamiento inicial para todos, y se sigue con las iniciativas de concientización en seguridad para mantener las defensas de la ingeniería social en la mente de todos. Se debe alinear el entrenamiento y concientización con políticas de seguridad específicas; es posible también tener una política de concientización y entrenamiento de seguridad.

Las siguiente técnicas pueden afianzar el contenido de un entrenamiento:

- Orientación a los nuevos empleados, almuerzos de entrenamiento, correos, noticias.
- Un documento de supervivencia sobre ingeniería social con sugerencias y FAQs
- Protectores de pantalla, mouse, pads, notas, lapiceros y posters en la oficina con mensajes para fortaleces los principios sobre seguridad.

MILE-SEC
Capacitación y Consultoría en Hacking Ético & Forense Digital

Webinar Gratuito
Ingeniería Social

Alonso Eduardo Caballero Quezada

Consultor e Instructor en Hacking Ético y Forense Digital

e-mail: ReYDeS@gmail.com

Diciembre 2018